

Myth Busting & Facts on the Proposed Regulation on Child Sexual Abuse: Addressing Privacy Concerns with Data and Facts

This document provides an overview of the main myths and concerns surrounding the proposed EU Regulation to prevent and combat child sexual abuse (CSA). It brings together evidence, research and factual analysis to address these concerns, with the aim of supporting an informed, evidence-based assessment of the proposed Regulation.

The Myths

- **Myth 1:** [The CSA Regulation will legalise mass surveillance and ‘read’ all our messages.](#)
- **Myth 2:** [The CSA Regulation will create a slippery slope, allowing governments to surveil political opponents or human rights defenders.](#)
- **Myth 3:** [The CSA Regulation will mean breaking encryption, including end-to-end encryption.](#)
- **Myth 4:** [Detecting new CSAM will lead to many false positives.](#)
- **Myth 5:** [A new Regulation is not necessary, extending the interim regulation is enough.](#)
- **Myth 6:** [The Digital Services Act \(DSA\) already protects children online, so there is no need for the CSA Regulation.](#)
- **Myth 7:** [Detection should only take place where there is already suspicion of illegal activity.](#)

The Facts

- **Fact 1:** [Automated detection is effective and essential in preventing the spread of CSAM. Public reporting will never be sufficient alone.](#)
- **Fact 2:** [Detecting new CSAM and grooming saves children in urgent need of rescue.](#)
- **Fact 3:** [There will be strong oversight and safeguard mechanisms on the CSA Regulation.](#)
- **Fact 4:** [Technology already exists to tackle child abuse while respecting privacy.](#)
- **Fact 5:** [Most child sexual abuse occurs in private messaging.](#)
- **Fact 6:** [Citizens overwhelmingly back the proposed CSA Regulation.](#)

*The [European Child sexual abuse Legislation Advocacy Group \(ECLAG\)](#) is a coalition of over 80 child rights organisations joining forces to protect children from sexual violence and abuse. The Steering Group of the Coalition is formed by [ECPAT International](#), [Eurochild](#), the [Internet Watch Foundation \(IWF\)](#), [Missing Children Europe](#), [Terre des Hommes Netherlands](#) and [Thorn](#).

The Myths

Myth 1: The CSA Regulation will legalise mass surveillance and 'read' all our messages.

This claim builds on a) misinterpretation of the process established by the proposed Regulation and b) misunderstanding of the technology at hand.

Under the proposed CSA Regulation, detection of (potential) child sexual abuse material would only happen **after a thorough process** of risk assessment, reviews, multiple checks and a court order, **making it virtually impossible for the detection technology to be misused** (see [Fact 2](#)).

The impact on users' privacy (see also [Myth 2](#)) would be a central consideration. The proposed CSA Regulation requires that any detection technology be the least privacy-intrusive measure capable of achieving its objective and as reliable as possible, minimising the risk of errors or false positives.

Detection technology is built for the sole purpose of detecting illegal material and grooming patterns. A computer processes data according to rules and algorithms. **It does not comprehend meaning, intent, context, or emotion.** It does not "read", understand, or store messages. **It looks for patterns** based on what it is trained on. An analogy is a metal detector: it can detect only metal and cannot identify or flag anything else that may be buried underground.

Myth 2: The CSA Regulation will create a slippery slope, allowing governments to surveil political opponents or human rights defenders.

Detection technologies are designed for one purpose only: to identify child sexual abuse material or recognise indicators of child grooming. They are not designed to monitor people's communications or conduct general surveillance. Repurposing these technologies for indiscriminate monitoring of all communications would be technically impossible, unrealistic and unlawful under the proposed CSA Regulation.

These technologies have been used successfully for more than a decade to help identify children at risk and remove illegal material from the internet. They are highly targeted, accurate, and operate in the background of online services without disrupting the experience of the overwhelming majority of users.

Detection technologies could only be deployed where all of the following conditions are met:

- **A high risk has been identified:** Detection may only be ordered for the specific part of a service that presents a high risk of being used for online child sexual abuse.
- **Other measures have proved insufficient:** Providers must first implement appropriate risk mitigation measures. Detection can only be ordered where they are not sufficient to address the identified risk.

- **An independent authority authorises it:** Detection requires a time-limited detection order issued by a judicial or independent administrative authority.
- **Approved technology is used:** Only technologies approved by the EU Centre as effective and privacy-preserving may be deployed.
- **Strict limits apply:** Detection orders are targeted, proportionate and limited in duration, with ongoing oversight and review (see [Fact 2](#)).

Taken together, these safeguards create a **high legal threshold for the use of detection technologies** and ensure they can only be deployed for the specific purpose of combating online child sexual abuse.

Myth 3: The CSA Regulation will mean breaking encryption, including end-to-end encryption.

The proposed CSA Regulation does not require encryption to be weakened, bypassed or removed. Nor does it require providers to create 'back doors' that would compromise the security of users' communications.

The Regulation is technology neutral. It does not mandate any specific technology for detecting child sexual abuse. Instead, it sets strict legal requirements that any detection technology must meet, including that it is as accurate as possible, has the least intrusive impact on users' rights, and respects privacy before it can ever be authorised for use.

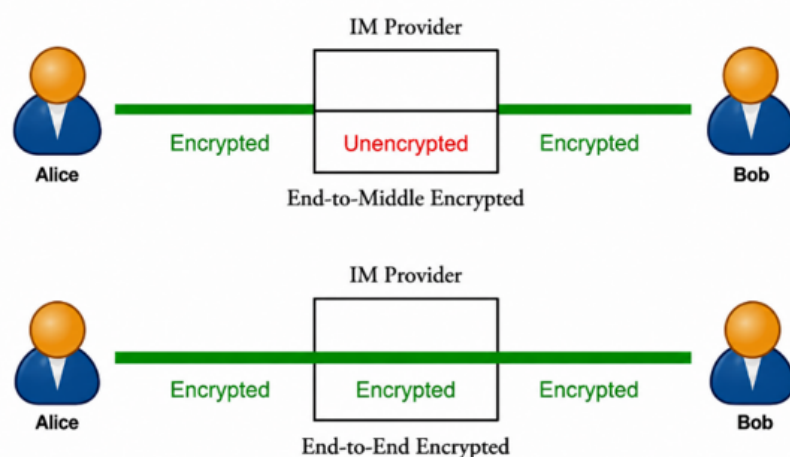
This approach allows the law to remain effective as technology evolves. Rather than prescribing a single technical solution, it defines the safeguards that any solution must satisfy.

One example is client-side scanning, sometimes called [upload prevention](#). This analyses content before it is encrypted and transmitted. **Because detection takes place before encryption is applied, the encryption itself is not weakened or broken.**

[Client-side scanning](#) is only one possible approach. Other privacy-preserving technologies – including [homomorphic encryption](#), secure [multi-party computation](#) and trusted execution environments ([secure enclaves](#)) – can also support the detection of child sexual abuse while minimising access to users' communications. As these technologies continue to develop, further privacy-preserving solutions are likely to emerge.

Privacy-preserving security checks are already widely used for other purposes.

This approach is not new. Similar privacy-preserving technologies are already **widely deployed** for other purposes. For example, [WhatsApp](#) detects and blocks [malicious URLs](#) before they are shared



without compromising end-to-end encryption; web browsers such as Chrome and [Microsoft Edge](#) check websites against lists of known malicious domains to warn users about phishing and malware; and [Apple's](#) Communication Safety feature analyses images on a child's device to warn about sensitive nude content before it is viewed or shared. When [Facebook Messenger](#) was end-to-end encrypted, Meta detected nudity for teens' accounts.

Myth 4: Detecting new CSAM will lead to many false positives.

Known CSAM - content that has already been flagged as illegal material and added to a secure database - is detected using hash matching. A hash is a unique digital fingerprint of an image or video. This technique allows systems to compare content being uploaded to a system against databases of known CSAM and identify exact or near-identical matches.

Detecting **new or previously unknown CSAM**, as well as grooming behaviour, requires different technologies. These use machine learning classifiers trained on datasets containing confirmed child sexual abuse material, adult pornography and legal imagery so they can distinguish illegal content and behaviour from benign material, such as family photographs of children. Companies can configure these systems to operate with very high confidence [thresholds](#), minimising false positives.

Once content is flagged by detection technology, **human review** – with analysts trained to identify illegal content – will confirm that the content is criminal, ensuring that only illegal material is acted on by law enforcement authorities.

To avoid false positives, specific threshold and accuracy requirements will be set by the EU Centre to ensure that high standards are met. Under the proposal for the CSA Regulation, the EU centre will assess the reports received to ensure only appropriate reports are shared with law enforcement authorities.

Myth 5: A new Regulation is not necessary as extending the Interim Regulation is enough.

From 2021 to 2026, the [Interim Regulation](#) (EU) 2021/1232 from certain provisions of the ePrivacy Directive provided a legal basis for providers of number-independent interpersonal communications services, such as webmail and chat services, to continue **voluntarily** detecting, reporting, and removing child sexual abuse on their platforms.

The extension of the temporary derogation alone would not be sufficient to address the scale of the current situation online. Children have the right to be protected equally on all the online platforms they use.

Even with a new regulation, there must be a **clear legal basis for voluntary detection** to ensure there are no gaps in child protection. A gap could occur, for example, if an online service provider has to wait to “fail” the risk assessment and mitigation process to receive a detection order to have the legal basis to find and block illegal content circulating on their services.

Myth 6: The Digital Services Act (DSA) already protects children online, so there is no need for the CSA Regulation.

The [Digital Services Act](#) is an important part of the EU's digital rulebook, but it was never designed to tackle online child sexual abuse comprehensively.

The DSA has a broader mandate and focuses on creating safer online services by requiring platforms to assess and mitigate systemic risks, remove illegal content when they become aware of it, and provide greater transparency and accountability. However, it does not create a legal framework for providers to proactively detect child sexual abuse material or the grooming of children, nor does it establish harmonised obligations to report identified abuse to the relevant authorities.

The CSA Regulation addresses these specific gaps. It would create a dedicated framework for preventing, detecting, reporting and removing online child sexual abuse, including both already identified as well as undiscovered child sexual abuse material and, where justified, the solicitation of children (grooming). It also establishes common EU rules, safeguards and oversight to ensure that detection measures are targeted, proportionate and subject to judicial or independent authorisation.

Myth 7: Detection should only take place where there is already suspicion of illegal activity.

While targeted investigations based on suspicion are an essential part of usual law enforcement operations, they are not sufficient to tackle online child sexual abuse.

The scale of offending online means that authorities cannot rely solely on pre-existing suspicion. Millions of images and videos of child sexual abuse material are shared online each year, often across a vast number of services and by offenders who have never previously come to the attention of police. Grooming offences are similarly hidden, taking place in private communications where there is often no victim report or other indication that abuse is occurring.

In many cases, there is no prior evidence that a particular user or service is being used to facilitate child sexual abuse. Providers often become aware of abuse only because detection technologies identify known CSAM, detect highly likely new CSAM, or identify patterns consistent with grooming. Without these tools, there may be no basis for suspicion in the first place.

NCMEC's 2025 CyberTipline data shows that the CyberTipline received 21.3 million reports in 2025. Of these, 21,181,300 came from electronic service providers, while only 170,193 came from the public. **This means that, for every 1 public report, there were about 124 reports from electronic service providers.** The child-safety system depends on platforms being able to detect and report at scale, under clear rules and strong safeguards.

A system that relies solely on pre-existing suspicion would therefore miss a significant amount of abuse.

The Facts

Fact 1: Automated detection is effective and essential in preventing the spread of CSAM. Public reporting alone will never be sufficient.

Public reporting is essential for identifying both known and previously unknown child sexual abuse material, but it will never be sufficient on its own due to the significant barriers to reporting. Many victims are unaware that their abuse has been recorded or shared online, some are too young to disclose what has happened to them, and older children may remain silent because of shame, fear, trauma or threats from the offender. Evidence consistently shows that child victims are unlikely to report abuse. One [prevalence study](#) found that 83% of young people aged 11 to 17 who had been sexually assaulted by a peer had not told anyone.

Equally, individuals who are deliberately sharing CSAM with others are highly unlikely to report themselves for illegal activity.

Proactive detection is essential to identify abuse that would otherwise remain hidden. The effectiveness of detection is demonstrated by what happens when it is removed. During the legislative gap in 2021, Meta suspended its voluntary detection activities in the EU for approximately 10 months, resulting in a [58% reduction](#) in reports of CSAM. This illustrates that pausing automated detection directly reduces the amount of abuse that is identified, reported and removed.

The [Internet Watch Foundation](#) (IWF), Europe's largest hotline, assessed 451,210 reports in 2025, confirming [311,610 reports](#) containing or leading to CSAM and adding more than 317,000 new images and videos to its hash list. 64% of all actioned reports resulted from the IWF's [proactive searching](#), demonstrating the value of proactive detection in identifying substantially more CSAM than public reporting alone. By comparison, externally submitted reports accounted for just 7% of all actioned reports.

Fact 2: Detecting new CSAM and grooming saves children in urgent need of rescue.

Behind every image and video of child sexual abuse, there is a child in danger. Detecting new child sexual abuse material and grooming is crucial to rescue children.

Online service providers in Europe already voluntarily use detection technologies to find and report child sexual abuse to the [The National Center for Missing and Exploited Children](#) (NCMEC) in the United States. NCMEC refers these reports to the relevant national law enforcement agencies, who can open inquiries to investigate and arrest perpetrators where a significant evidence threshold has been reached. The detection and reporting of new CSAM enables police to rescue children and arrest offenders every day. In the UK alone, an estimated [1,200 children safeguarded and 800 suspected child sex offenders arrested](#) on average every month.

Proactive detection and blocking is also crucial to prevent [re-victimisation](#). The redistribution of any type of abuse material means that, for victims, the abuse not only stays in their memory, but is constantly re-lived. It is widely acknowledged that the trauma of having child

sexual abuse material recirculating is extremely damaging, creating difficulties for victims to heal from their abuse. Children exposed to grooming and sexually explicit content report [similar levels of trauma symptoms](#) (i.e. clinically diagnosable PTSD) to victims of penetrative offline sexual offences.

Fact 3: There will be strong oversight and safeguard mechanisms on the CSA Regulation.

The Regulation will not permit the indiscriminate scanning of private messages. It will establish strong **safeguards and a long review process** before any detection is authorised to ensure that **no indiscriminate detection** of illegal material is carried out and to minimise any invasion of privacy.

These safeguards are likely to include:

- Detection technologies will be authorised and provided by the EU Centre. Online service providers will not be able to use detection technology that infringes the minimum standards of security and privacy established by the Centre and the Regulation.
- Detection orders will be issued by a national judicial or administrative authority, in line with national and EU law on data protection and fundamental rights.
- National Coordination Authorities will review and give feedback on the risk management and on the implementation plan of a detection order.
- Data Protection Authorities can also provide recommendations in the detection process.

Multiple checks, including from the EU Centre and a Data Protection Authority, transparency reporting and oversight, are foreseen to ensure that the detection conforms to EU law, including the GDPR, and respect the privacy of users.

- **The Regulation must comply with existing EU law.** Like all EU legislation, the proposed CSA Regulation must comply with the EU Charter of Fundamental Rights and the GDPR, meaning any processing of personal data must be lawful, necessary and proportionate.
- **Detection technologies must meet strict legal standards.** The Court of Justice of the European Union has recognised that targeted automated filtering can be compatible with EU law where it is sufficiently accurate, proportionate and accompanied by appropriate safeguards.
- **Independent authorities – not platforms – authorise intrusive measures.** Decisions that require providers to detect child sexual abuse are made by independent judicial or administrative authorities, rather than left to the discretion of individual companies.
- **Technology does not make the final decision.** Any content flagged by detection technologies is subject to verification to confirm that it constitutes illegal child sexual abuse material before action is taken.
- **Providers must be transparent about their actions.** The Regulation requires platforms to be transparent about the measures they use to detect, report and remove child sexual abuse, enabling public scrutiny and accountability.
- **Detection databases are independently managed.** The databases of indicators (such as hashes and other detection tools) used to identify known and new CSAM

and online grooming are created, maintained and operated by the EU Centre, not by technology companies or national law enforcement authorities.

- **The Regulation includes robust oversight and safeguards.** Detection measures are subject to legal authorisation, independent oversight, transparency requirements and safeguards designed to protect users' fundamental rights while ensuring children are protected from sexual abuse online.

Fact 4: Technology already exists to tackle child abuse while respecting privacy.

Technologies already exist that effectively detect CSAM with high accuracy rates. Those include [PhotoDNA](#), [YouTube CSAI Match](#), [Facebook's PDQ and TMK+PDQF](#) for known CSAM and [Thorn's Safer Tool](#), [Google's Content Safety API](#) and Facebook's AI Technology, for new or unknown CSAM and grooming. Those technologies are already deployed at scale with no issue of misuse or privacy concerns.

[Upload prevention](#) or client-side scanning is already deployed at scale in end-to-end encrypted environments for legitimate purposes, such as preventing the spread of viruses or malware. Online service providers, including [Apple](#), already use it to flag CSAM and grooming conversations in their messaging apps. Detecting CSA in these environments could be executed using the same technology (see [Myth 5](#) and [Myth 3](#)).

The Regulation will provide a framework to ensure the technology used to detect CSAM and grooming minimises intrusion in private spaces. This will be evaluated by the opinion of experts and judicial courts, whose job it will be to make sure the detection is targeted, effective, and proportionate (see [Fact 3](#)). The Regulation will give industry a powerful incentive to develop further their suite of privacy-preserving detection technologies across the different parts of their services.

The privacy of all users is extremely important. Children, victims and survivors have a right to privacy too. Their privacy is currently being violated on a ginormous scale as pictures and videos of the worst moments of their lives are shared, sold, and traded online.

Fact 5: Most child sexual abuse occurs in private messaging.

Private messaging services are the primary environment in which perpetrators groom children and share child sexual abuse material. [Research](#) shows that two-thirds of children who received sexually explicit material online did so through private messaging, most commonly on their personal phone.

This is why effective child protection measures must extend to private messaging services. Detection technologies deployed in these environments help identify known and new CSAM, as well as patterns of grooming behaviour, enabling providers to intervene, report abuse and safeguard children. Contrary to some claims (see [Myth 1](#)), these technologies cannot “read” or understand the content of messages in the way a human would. Instead, they use highly targeted, privacy-preserving techniques to identify indicators of child sexual abuse.

It is well recognised that perpetrators routinely use a tactic known as “[off-platforming](#)”. This means they initiate contact with children on public platforms before persuading them to move

to private messaging services – particularly those offering end-to-end encryption or lacking detection capabilities – where they believe they are less likely to be identified. Excluding private messaging from the scope of the CSA Regulation would create a significant enforcement gap and risk turning these services into safe havens for offenders.

Protecting children online requires measures that address where abuse actually occurs. Limiting detection to public-facing services would leave the environments most commonly used to groom children and distribute CSAM beyond the reach of effective child protection measures.

Fact 6: Citizens overwhelmingly back the CSA Regulation.

In 2025, analysts at the Internet Watch Foundation reviewed [196,101 webpages hosted in the EU containing child sexual abuse material](#). This figure represents [63% of CSAM URLs](#). Europeans are aware that child sexual abuse is a rising problem in their countries and there is overwhelming support for online service providers to proactively fight against this crime.

A 2023 [Eurobarometer survey](#) showed that 78% of respondents approve of the European Commission's legislative proposal to prevent and combat child sexual abuse and 96% see the ability to detect child abuse equally as important or more important than the right to online privacy. Moreover, between 84% and 89% support the idea that service providers use tools to automatically detect images and videos of already known CSAM (89%), new images and videos (85%) and grooming (84%).

Similarly, a [recent ECPAT and NSPCC poll](#) proved that 81% of European respondents support obliging online service providers to detect, report, and remove child sexual abuse online. Data reveals that the majority of polled EU citizens see online service providers as one of the most important actors in preventing and protecting children from sexual abuse and exploitation online. 95% said that it is key that there are regulations to prevent online child sexual abuse.

An [IWF poll](#) of more than 6,000 adults in [Germany](#), [Italy](#) and [Poland](#) in October and November 2025 showed that 88% of respondents want their respective governments to back the CSAR. More than eight in 10 adults say they also support the CSAR that could see companies proactively detect and block images and videos of children being sexually abused online.

These findings underline a critical message: European citizens are deeply concerned about the child sexual abuse crisis unfurling online.

More than half of all Europeans surveyed declare that the issue of child sexual abuse and exploitation online will influence how they vote at a future election. There is a clear and urgent demand for decisive action to address this issue.